

```

RecipientInfo ::= CHOICE {
    ktri KeyTransRecipientInfo,
    kari [1] KeyAgreeRecipientInfo,
    kekri [2] KEKRecipientInfo }

KeyTransRecipientInfo ::= SEQUENCE {
    version CMSVersion, -- always set to 0 or 2
    rid RecipientIdentifier,
    keyEncryptionAlgorithm KeyEncryptionAlgorithmIdentifier,
    encryptedKey EncryptedKey }

RecipientIdentifier ::= CHOICE {
    issuerAndSerialNumber IssuerAndSerialNumber,
    subjectKeyIdentifier [0] SubjectKeyIdentifier }

```

FIG. 5B

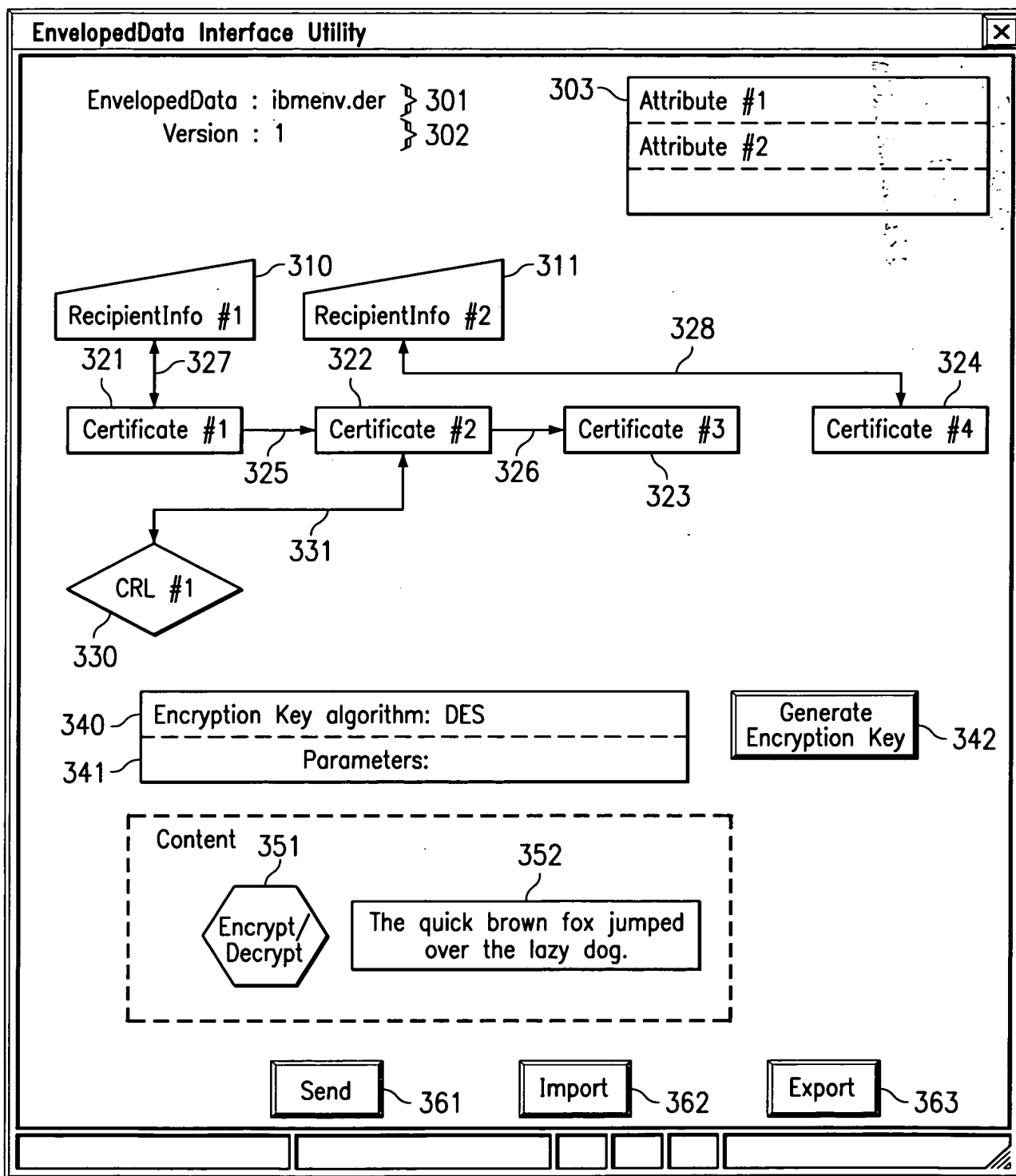


FIG. 3

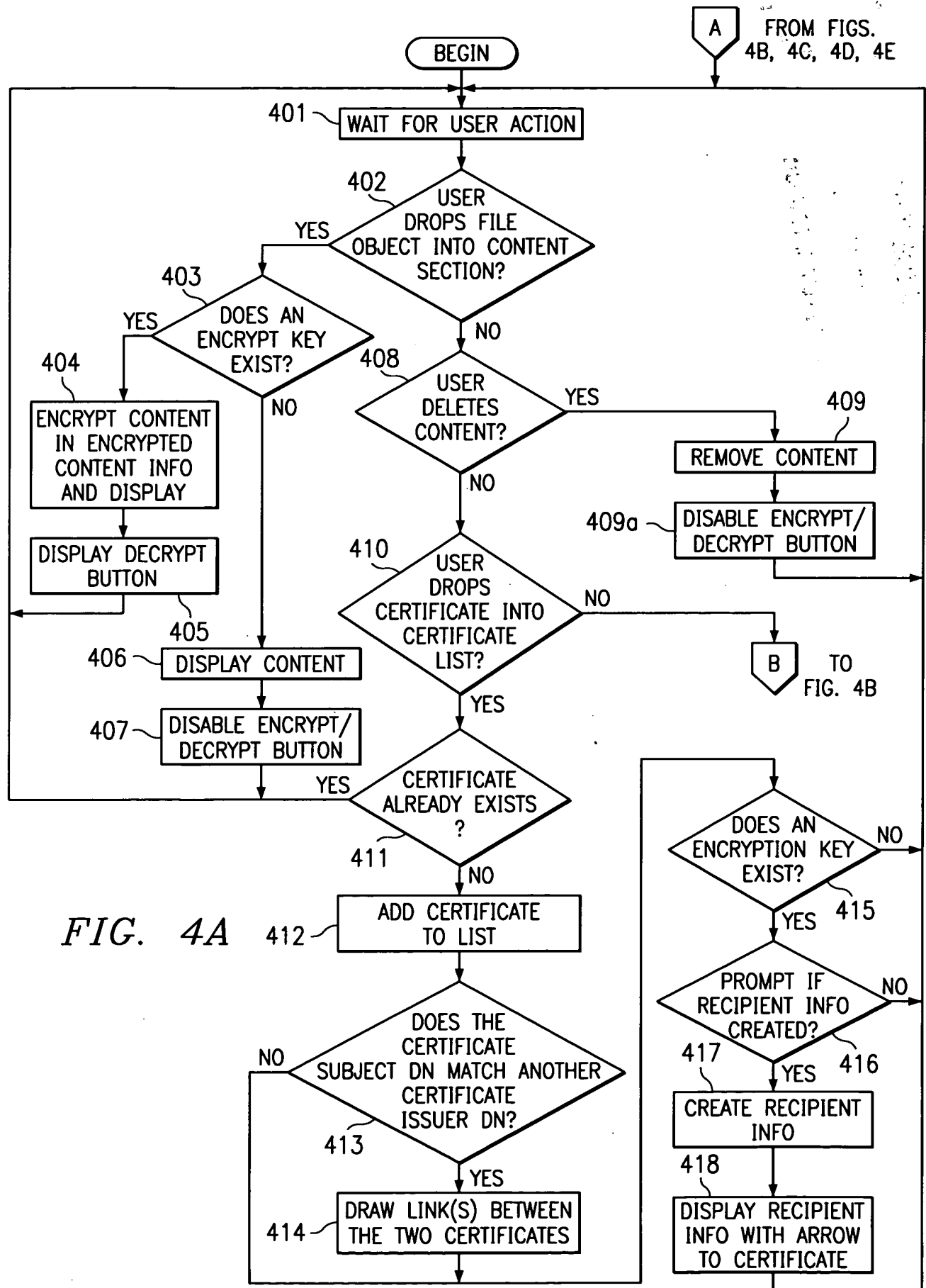


FIG. 4B

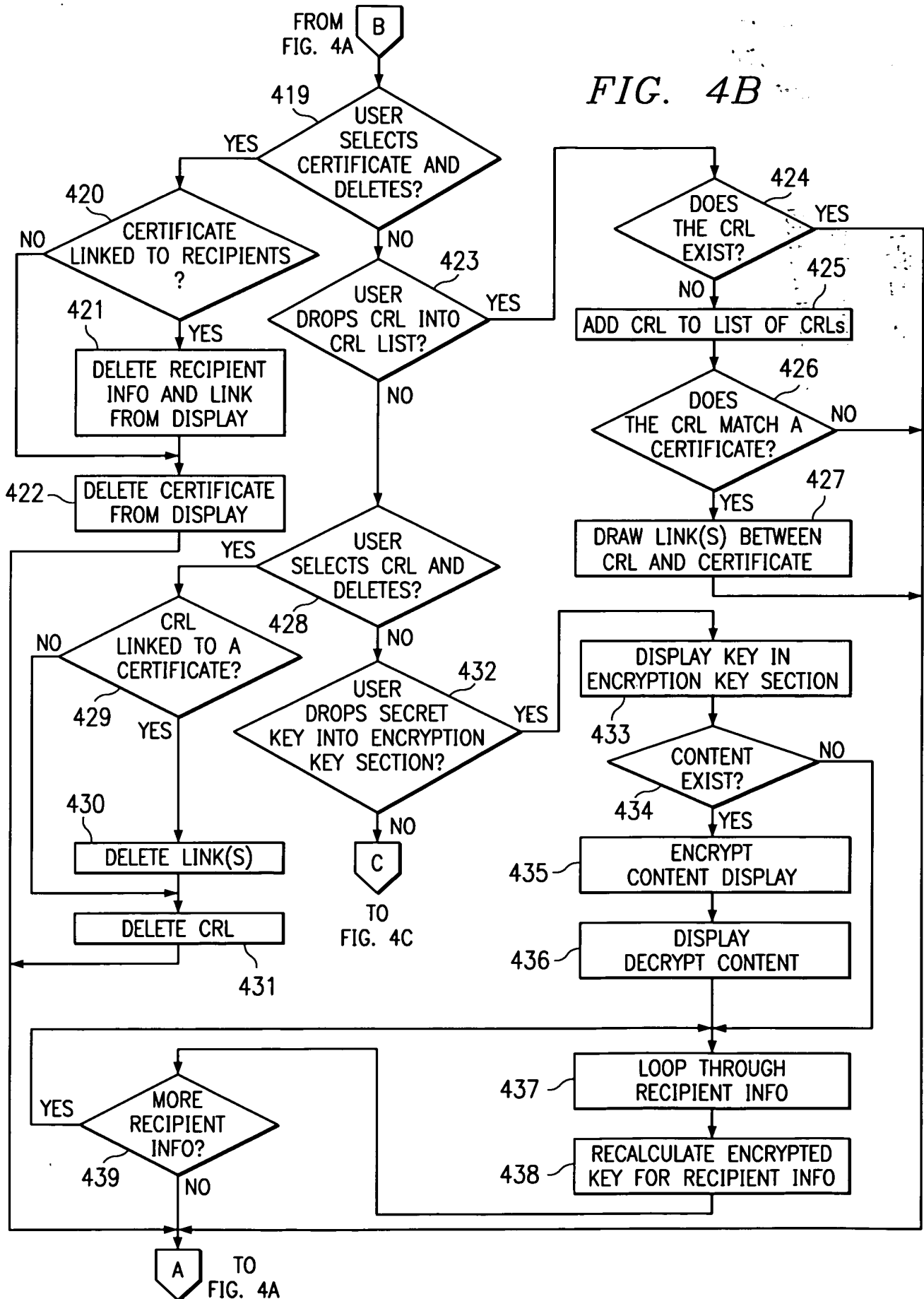
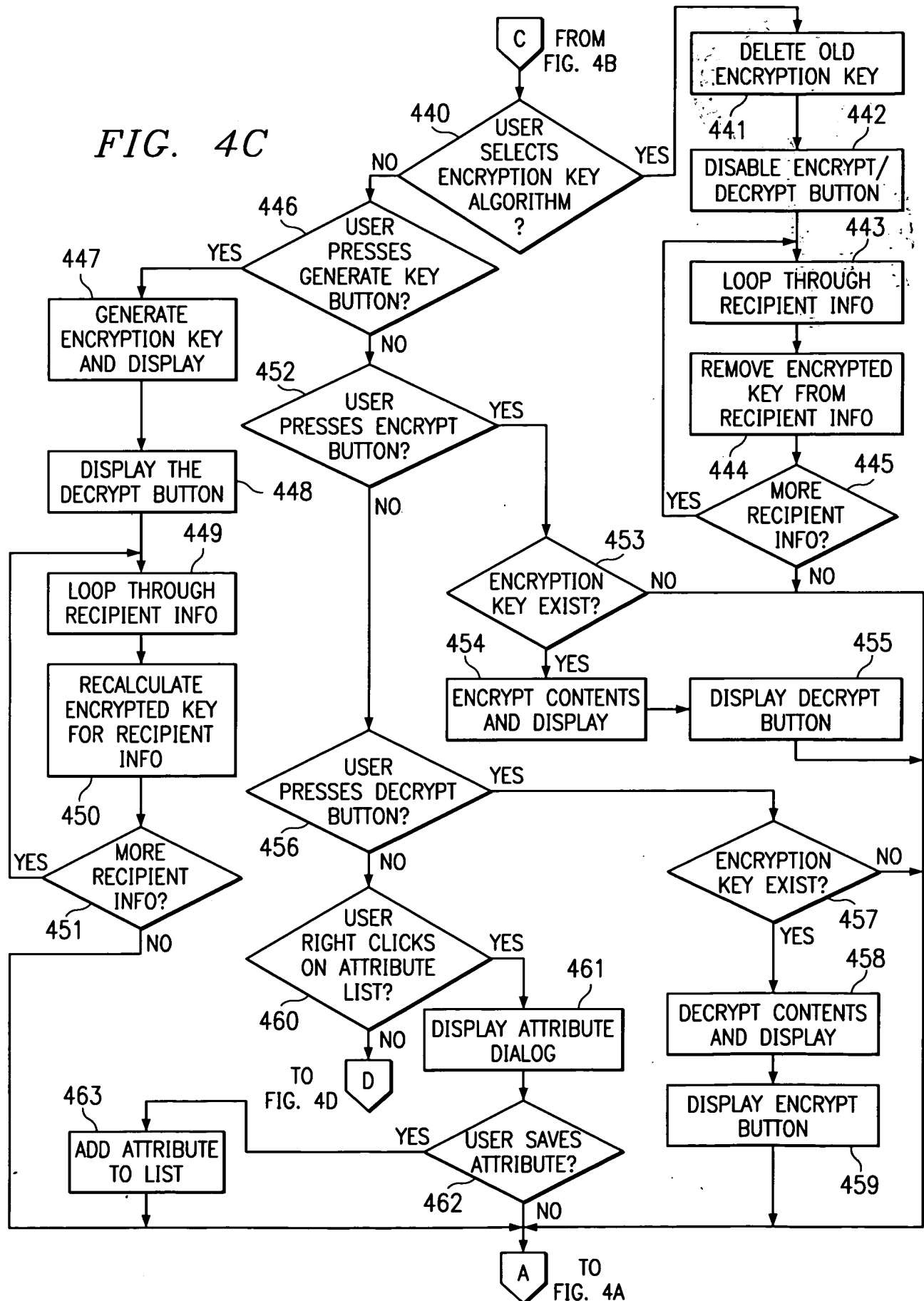
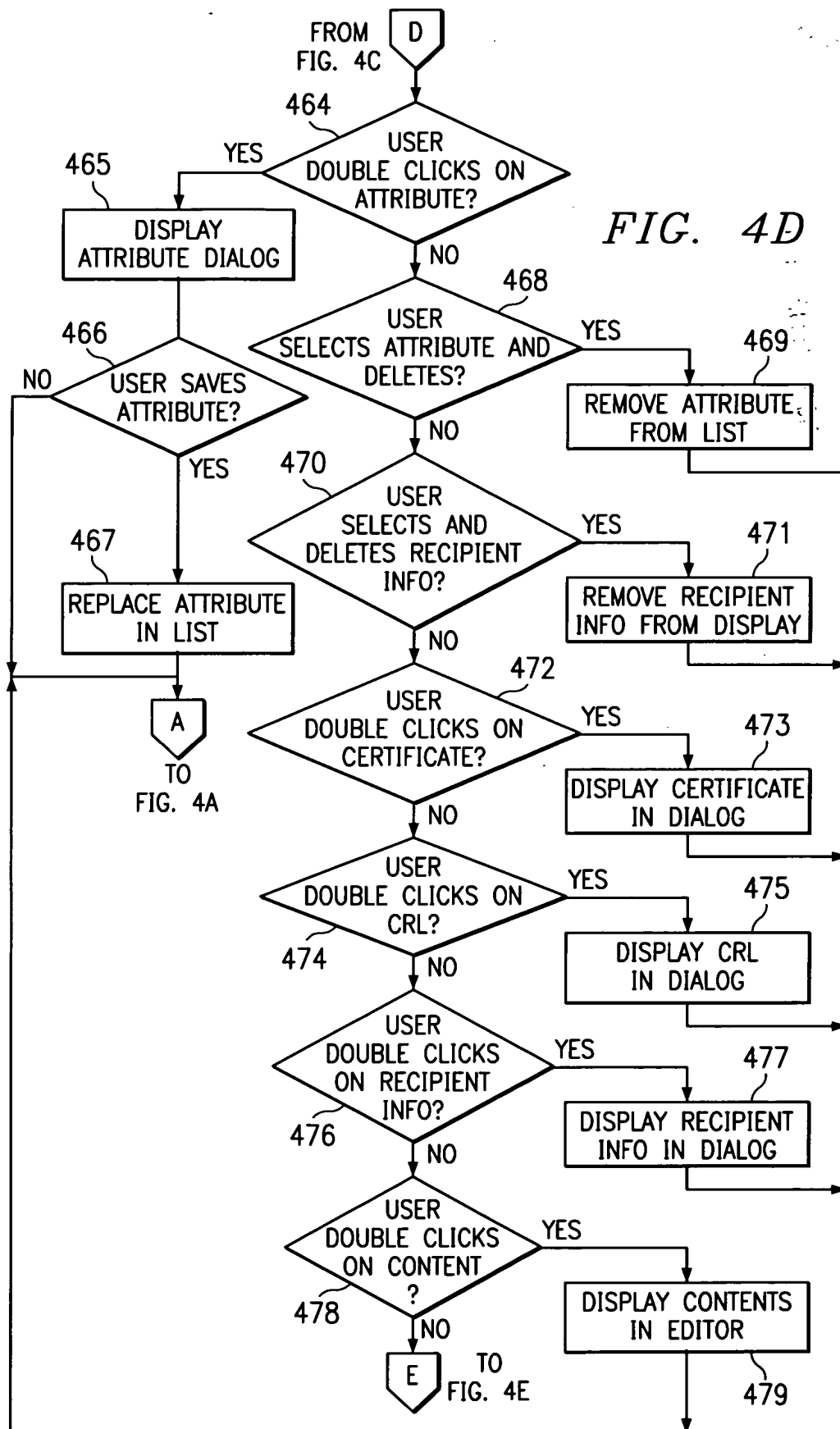
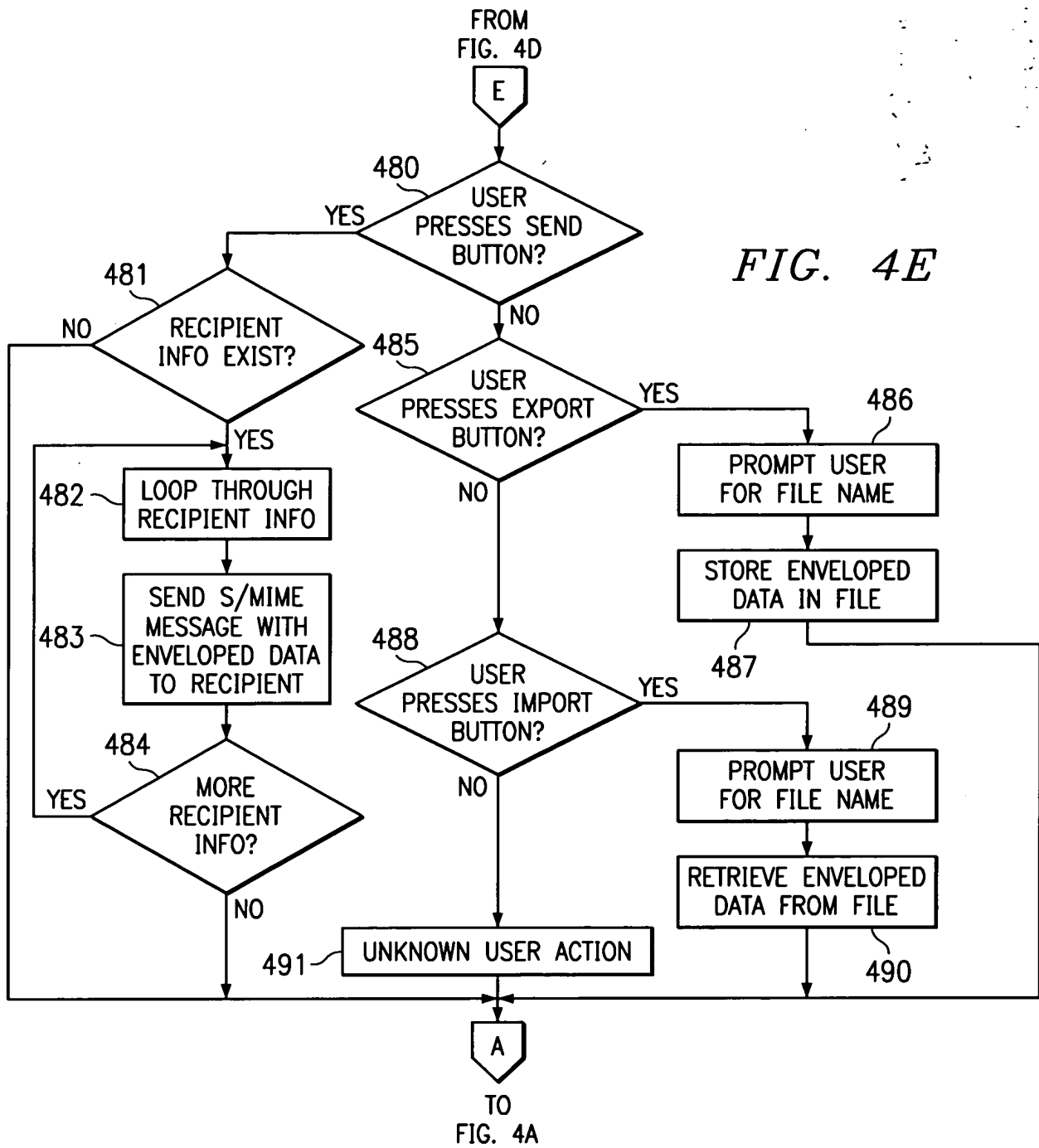
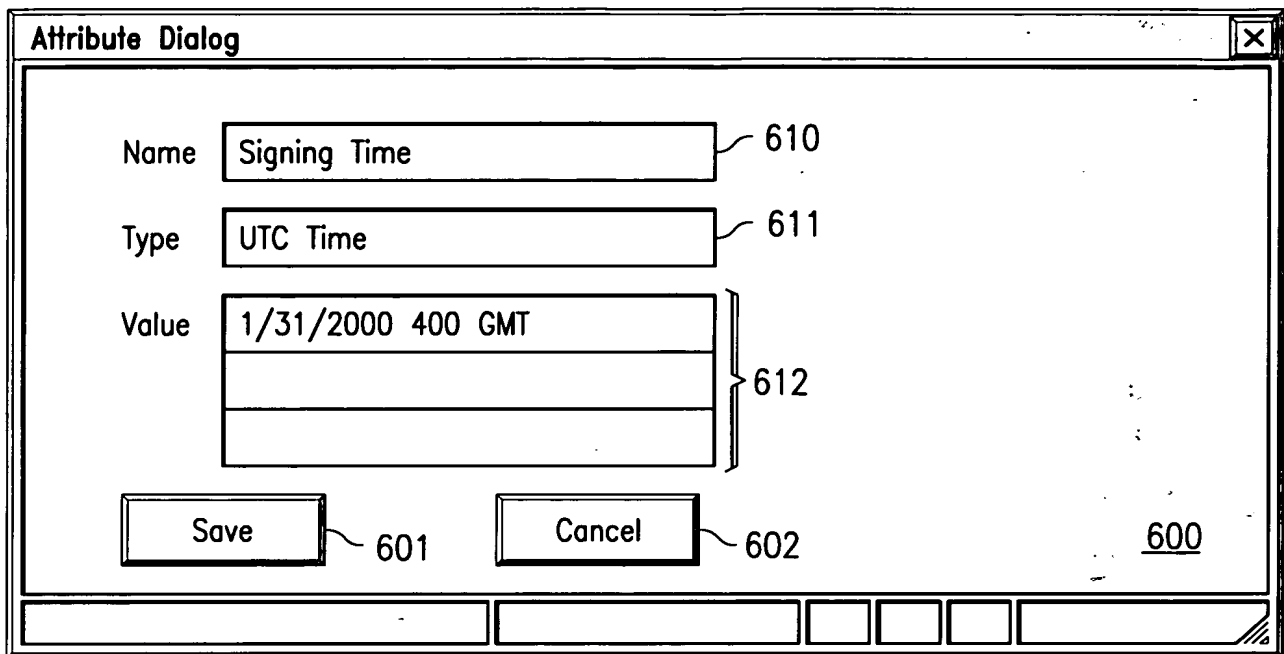


FIG. 4C





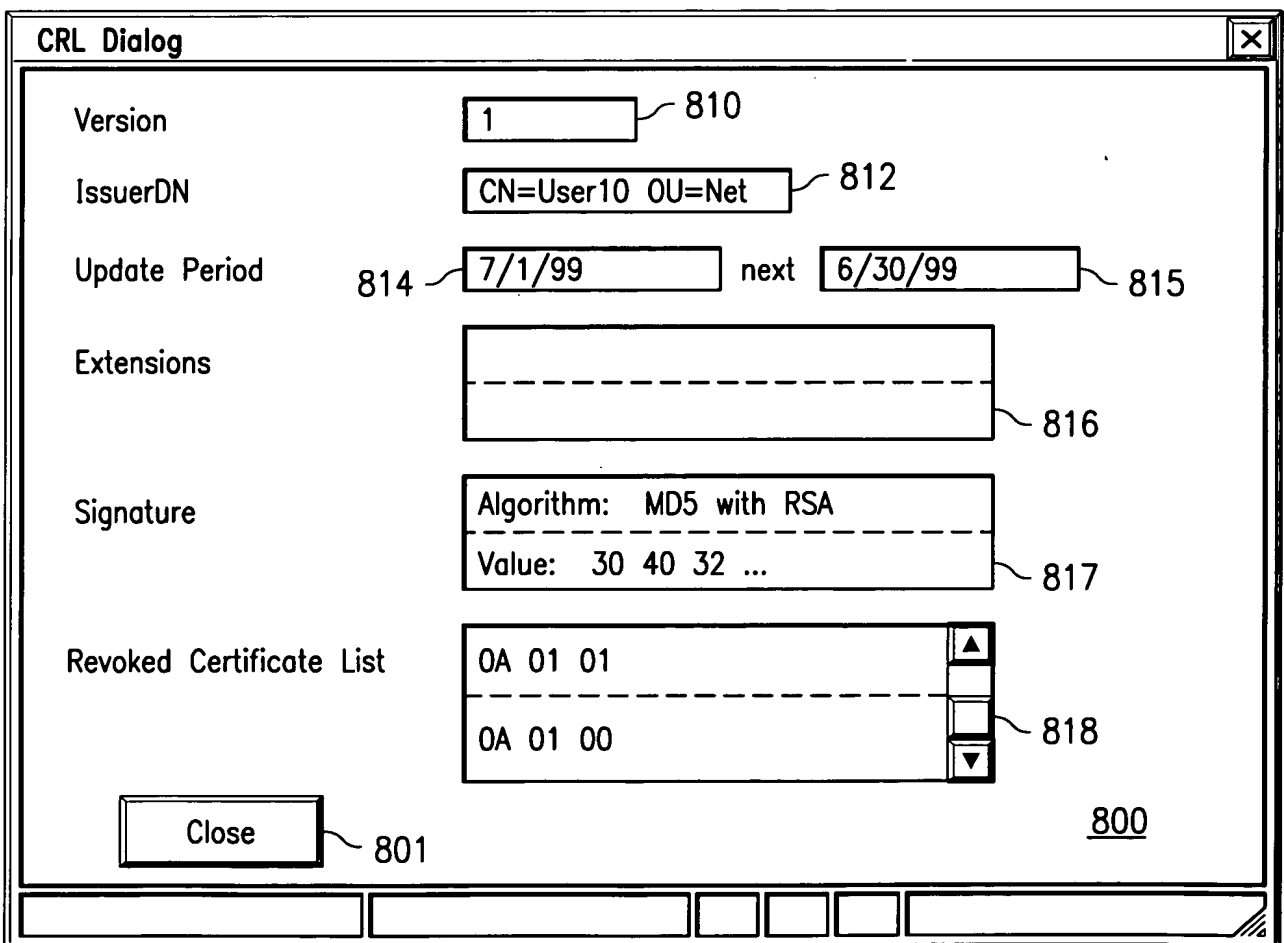




The 'Attribute Dialog' window contains the following elements:

- Name:** A text field containing 'Signing Time' (labeled 610).
- Type:** A text field containing 'UTC Time' (labeled 611).
- Value:** A multi-line text area containing '1/31/2000 400 GMT' (labeled 612).
- Buttons:** 'Save' (labeled 601) and 'Cancel' (labeled 602).
- Reference:** A label '600' is located in the bottom right corner of the dialog area.

FIG. 6



The 'CRL Dialog' window contains the following elements:

- Version:** A text field containing '1' (labeled 810).
- IssuerDN:** A text field containing 'CN=User10 OU=Net' (labeled 812).
- Update Period:** Two date fields. The first contains '7/1/99' (labeled 814) and the second contains '6/30/99' (labeled 815), separated by the word 'next'.
- Extensions:** A text area containing a dashed line (labeled 816).
- Signature:** A text area containing 'Algorithm: MD5 with RSA' and 'Value: 30 40 32 ...' (labeled 817).
- Revoked Certificate List:** A list box containing '0A 01 01' and '0A 01 00' (labeled 818), with up and down arrow buttons.
- Buttons:** A 'Close' button (labeled 801).
- Reference:** A label '800' is located in the bottom right corner of the dialog area.

FIG. 8

Certificate Dialog [X]

Version	3	710
Serial Number	31 40 60 14 ...	711
IssuerDN	CN=User1 OU=Net	712
Issuer Serial Number	40 31 14 56 ...	713
SubjectDN	CN=Signer OU=Net	714
Validity Period	12/01/1999 to 11/30/2000	715 716
Public Key	Algorithm: RSA Value: 30 16 40 12 ...	717
Signature	Algorithm: MD5 with RSA Value: 30 20 18 36 ...	718
Extended Attributes	Algorithm: Policies 5 Value: Basic Constraints	719

Private Key 720

Close 701

700

FIG. 7